frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 22 August 2022
DOI 10.3389/fphy.2022.981376

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Run-hua Shi,
North China Electric Power University, China
Mingxing Luo,
Southwest Jiaotong University, China
Yuling Chen,
Guizhou University, China

*CORRESPONDENCE
San-Qiu Liu,
sqlgroup@ncu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 29 June 2022
ACCEPTED 15 July 2022
PUBLISHED 22 August 2022

CITATION
Wang B, Gong L-H and Liu S-Q (2022), Multi-party quantum private size comparison protocol with d-dimensional Bell states.
Front. Phys. 10:981376.
doi: 10.3389/fphy.2022.981376

Multi-party quantum private size comparison protocol with *d*-dimensional Bell states

Bing Wang[1,2,3], Li-Hua Gong[1,4] and San-Qiu Liu[1,2,3]*

[1]Jiangxi Province Key Laboratory of Fusion and Information Control, Department of Physics, Nanchang University, Nanchang, China, [2]School of Physics and Materials, Nanchang University, Nanchang, China, [3]NCU-ASIPP Magnetic Confinement Fusion Joint Lab, Institute of Fusion Energy and Plasma Application, Nanchang University, Nanchang, China, [4]Department of Electronic Information Engineering, Nanchang University, Nanchang, China

A feasible multi-party quantum private comparison (MQPC) protocol based on *d*-dimensional Bell states was proposed. In the protocol, all participants can independently encrypt their privacies and send them to a semi-honest quantum third party (TP) through authenticated channels. Then, the TP can determine the size relationship among all participants' privacies without gaining access to the private information. We verified correctness and effectiveness of the proposed protocol with some examples. In addition, compared with other similar protocols, it is not necessary to perform unitary operation on particles and only single-particle measurement is required. Furthermore, the relatively high qubit efficiency is promised. The security analysis verifies that the proposed protocol can counteract external and internal attacks in theory.

KEYWORDS

multi-party quantum private comparison, size relationship, *d*-dimensional bell state, qubit efficiency, semi-honest quantum third party

1 Introduction

Secure multi-party computation (SMC) was introduced by the famous Millionaires' problem in 1982 [1], where two millionaires want to compare their wealth and learn who is wealthier without revealing their actual property. With the combination of quantum mechanics and information science, researchers have found that processing information using quantum systems has led to many striking results, such as teleportation of quantum states and quantum algorithms that are exponentially faster than their known classical counterpart. Therefore, the quantum version of SMC has once again set off a research boom. As a particular instance of quantum SMC (QSMC), quantum private comparison (QPC) has wide applications in private bidding and auctions, secret ballot elections, commercial business, identification.

Right after Yao's millionaire problem, [2] designed an efficient and fair protocol to determine whether two millionaires are equal rich. However, as proved by [3], a quantum two-party secure computation is impossible. Therefore, a third party (e.g., a semi-honest third party) is often involved to help them achieve the task in a QSMC protocol. The semi-honest quantum third party (TP) will always follow the process of the protocol honestly.

He will not prepare other types of particles (e.g., GHZ state, single photon) and conspire with any participants or outside eavesdroppers to steal the participants' privacies. But the TP is curious to know the participants' privacies, and try to extract their private information from he knows.

In 2009, the first QPC protocol was proposed by based on Bell states [4]. With decoy particle technology, one-way hash function and unitary operation, this protocol can compare the equality. In 2010, [5] devised a novel QPC protocol to compare the equality based on GHZ states, where the unitary operation is necessary. These early QPC protocols can only compare the equality. In 2011, a new QPC protocol was presented by [6] to compare the size relationship of privacies, where the information of size was encoded into the phase of GHZ state. In 2013, Lin et al. also designed a protocol to compare the size relationship based on the d-dimensional Bell states [7]. However, the four QPC protocols mentioned above are only related to the comparison between two participants. These two-party protocols are by no means the end of the QPC research. In future secure quantum network communication, the MQPC protocol will play an important role.

Fortunately, in 2013, the first MQPC protocol was proposed based on GHZ states by [8]. Suppose there are N $(N \geq 2)$ participants, each of them has a privacy, then N participants can determine whether their privacies are the same or not with the assistance of the TP. In 2014, Luo et al. devised a novel MQPC protocol based on d-dimensional multi-particle entangled states [9]. In their protocol, N $(N \geq 2)$ participants' privacies can be sorted by size with the help of the TP, and decoy particles were used to check eavesdropping. In the same year, [10] presented two MQPC protocols in distributed mode and traveling mode respectively based on multi-particle entangled states. With the assistance of the TP, the two protocols can also compare the equality of privacies for N $(N \geq 2)$ participants. Since then, various two-party [11–13] and multi-party QPC protocols have been proposed [14–17]. In 2018, Ye et al. proposed two novel multi-party quantum private comparison protocols for size relation comparison by using d-level single-particle states. In 2021, Zhou et al. presented an efficient QPC protocol to compare the size relationship of privacies between two classical participants based on d-dimensional Bell states. It should be noted that many previous protocols involved many kinds of operations, such as quantum measurement, unitary operation, and hash function. What's more, some of them suffer from low qubit efficiency. Besides, only few MQPC protocols can compare the size relationship among the privacies.

To make the implementation of the protocol easier, a new MQPC protocol to compare the size relationship among many participants' privacies is proposed. The d-dimensional Bell states are taken as quantum resources and the TP is introduced to help participants to make private comparison. The rest of this paper is organized as follows: the proposed MQPC protocol based on the d-dimensional Bell state is detailed in Section 2. The correctness and security are analyzed in Section 3, Section 4, respectively. The comparisons of the proposed protocol and the similar QPC protocols are made in Section 5. Finally, a short conclusion is given in Section 6.

2 The proposed MQPC protocol based on d-dimensional bell states

Assume there are N participants (P_1, P_2, ..., P_N) and each participant P_n $(n \in \{1, 2, ..., N\})$ possesses a L-length privacy $p_n = p_n^1 p_n^2 ... p_n^L$ (if the numbers of some digits are less than L, then sufficient 0s are added to their highest digit), where, $p_n^l \in \{0, 1, ..., h-1\}$, $h = \frac{d+1}{2}$, and $l \in \{1, 2, ..., L\}$. In addition, there is a pre-shared key through a secure QKD protocol [18] among these participants denoted as $A = A^1 A^2 ... A^L$, $A^l \in \{0, 1, ..., h-1\}$. Via the help of TP, they want to compare their privacies by size without revealing any private information. Next, the d-dimensional Bell state will be reviewed first. Then, the detailed description of the proposed protocol will be given (Figure 1).

2.1 d-dimensional bell state

Bell state, used to describe the four maximal entangled states in two-qubit system, is the most basic quantum entangled state. Compared with other quantum entangled states, Bell state is the easiest to prepare in experiment. Therefore, Bell state is widely used to design quantum cryptographic protocol. In a d-dimensional Hilbert space, Bell state can be expressed as [19, 20]

$$|\psi_{u,v}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi iku}{d}} |k\rangle \otimes |k \oplus v\rangle \tag{1}$$

where $u,v \in \{0, 1, 2, ..., d-1\}$, and $\oplus$ denotes modulo d addition. Two indistinguishable orthogonal bases Z-basis $\bar{Z}$ and X-basis $\bar{X}$ in the d-dimensional quantum system are

$$\begin{aligned} \bar{Z} &= \{|j\rangle | j = 0, 1, ..., d-1.\} \\ \bar{X} &= \{F|j\rangle | j = 0, 1, ..., d-1.\} \end{aligned} \tag{2}$$

where $F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i}{d} kj} |k\rangle$ with $j = 0, 1, \ldots, d-1$represents quantum Fourier transform.

2.2 The proposed MQPC protocol

Step 1: According to Eq. 1, the TP randomly prepares $L \times N$ d-dimensional Bell states and they are

$$\begin{aligned} &|\psi_{u_1^1,v_1^1}\rangle, |\psi_{u_2^1,v_2^1}\rangle, ..., |\psi_{u_N^1,v_N^1}\rangle \\ &|\psi_{u_1^2,v_1^2}\rangle, |\psi_{u_2^2,v_2^2}\rangle, ..., |\psi_{u_N^2,v_N^2}\rangle \\ &\cdots \\ &|\psi_{u_1^L,v_1^L}\rangle, |\psi_{u_2^L,v_2^L}\rangle, ..., |\psi_{u_N^L,v_N^L}\rangle \end{aligned} \tag{3}$$

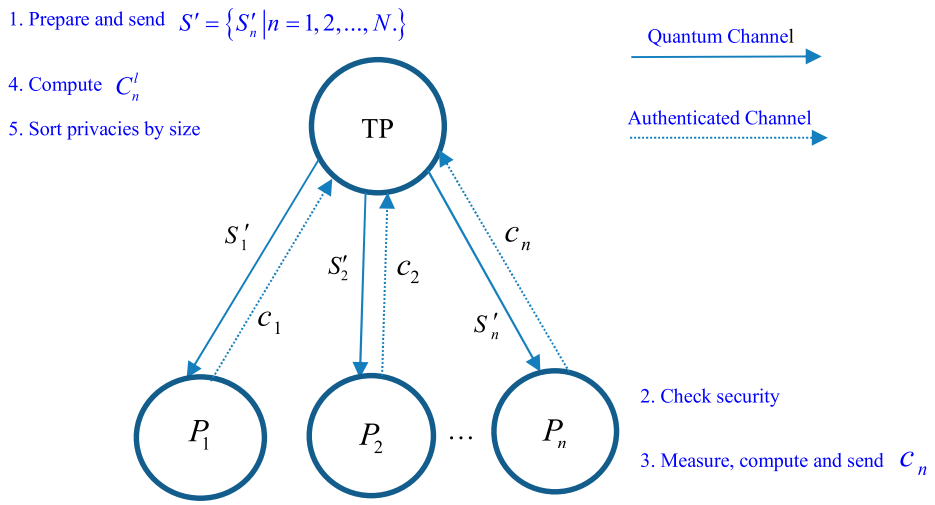

FIGURE 1
The schematic figure of the proposed protocol. The TP needs to implement steps 1, 4, 5 and each participant needs to implement steps 2, 3.

Based on these prepared Bell states in Eq. 3, he will record the v_n^l of each state and prepare $2N$ quantum sequences, namely $S = \{S_n | n = 1, 2, ..., N.\}$ and $T = \{T_n | n = 1, 2, ..., N.\}$, which contain all the first and second particles of the EPR pairs, respectively. Each particle-sequence contains L particles

$$S_n: [S_n^1, S_n^2, ..., S_n^L],$$
$$T_n: [T_n^1, T_n^2, ..., T_n^L].$$

To prevent eavesdropping, TP will prepare NL decoy particles randomly in $\bar{Z}$ or $\bar{X}$, and uniformly insert them into each sequence S_n to form a new sequence S_n'. Then, sequence S_n' is sent to participant P_n via a quantum channel, while all sequences $T = \{T_n | n = 1, 2, ..., N.\}$ are kept by the TP.

Step 2: After all the quantum sequences have been received by the corresponding participants, TP will announce the position and the measurement basis of each decoy particle in sequence S_n'. Then, each participant will check the security of the sequence received. Concretely, according to the announcement, each participant will use the right bases to measure these decoy particles and return the measurement results to TP. Then, the TP will verify these results and check whether eavesdroppers exist in the quantum channel. If the error rate is less than a predetermined threshold, the protocol will proceed to the next step; otherwise, the protocol will be terminated.

Step 3: After removing these decoy particles, each participant will measure the remaining particles with Z basis and record them as k_n^l. Then, he (she) will compute c_n^l,

$$c_n^l = k_n^l \oplus p_n^l \oplus A^l \tag{4}$$

Then, Participant P_n will obtain a sequence $c_n = c_n^1 c_n^2 ... c_n^L$ and send it to the TP via an authenticated channel.

Step 4: When confirming all sequences embedded privacy data have been received, TP will measure the particles in each sequence T_n and record them as t_n^l. Then, he will compute C_n^l,

$$C_n^l = c_n^l \oplus v_n^l \ominus t_n^l \tag{5}$$

Here, v_n^l is the record value in Step 1 and $\ominus$ denotes modulo d subtraction.

Step 5: After TP obtaining sequence $C_n = \{C_n^l | l = 1, 2, ..., L.\}$ from each participant, he will finish sorting the privacies by size. The TP takes out the same digits (the l-th digit) from sequences $C_1, C_2, \ldots, C_N$ and compute $R_{nn'}^l$,

$$R_{nn'}^l = C_n^l \ominus C_{n'}^l \tag{6}$$

Then, he can obtain $\text{sign}[R_{nn'}^l]$,

$$\text{sign}\left[R_{nn'}^l\right] = \begin{cases} 1, 0 < R_{nn'}^l \le h - 1; \\ 0, R_{nn'}^l = 0; \\ -1, h - 1 < R_{nn'}^l \le 2h - 2. \end{cases} \tag{7}$$

For the l-th elements of all participants' privacies $p_1^l, p_2^l, \ldots, p_N^l$, the TP can deduce their size relationship easily from $\text{sign}[R_{nn'}^l]$. that is

$$\text{sign}\left[R_{nn'}^l\right] = \begin{cases} 1, p_n^l > p_{n'}^l; \\ 0, p_n^l = p_{n'}^l; \\ -1, p_n^l < p_{n'}^l. \end{cases} \tag{8}$$

3 Correctness analysis

3.1 Output correctness

The quantum resource used in the protocol is the d-dimensional Bell state. According to the entanglement properties of Bell state, if one measures the particle with $\bar{Z}$, the d-dimensional Bell state will collapse into $|k\rangle|k \oplus v\rangle$. Therefore, the measurement results k_n^l and t_n^l satisfy the relationship, such that

$$k_n^l \oplus v_n^l = t_n^l \tag{9}$$

Therefore, based on Eqs 4, 5 and 6, the Eq. 9 can be deduced

$$\begin{aligned} R_{nn'}^l &= C_n^l \ominus C_{n'}^l \\ &= \left(c_n^l \oplus v_n^l \ominus t_n^l\right) \ominus \left(c_{n'}^l \oplus v_{n'}^l \ominus t_{n'}^l\right) \\ &= \left(k_n^l \oplus p_n^l \oplus A^l \oplus v_n^l \ominus t_n^l\right) \ominus \left(k_{n'}^l \oplus p_{n'}^l \oplus A^l \oplus v_{n'}^l \ominus t_{n'}^l\right) \\ &= \left(p_n^l \oplus A^l\right) \ominus \left(p_{n'}^l \oplus A^l\right) \\ &= p_n^l \ominus p_{n'}^l \end{aligned} \tag{10}$$

From Eq. 10, one can see that the value of $R_{nn'}^l$ indicates the size relationship between p_n^l and $p_{n'}^l$. Therefore, according to Eqs 7, 8 the TP can obtain the size relationship among the privacies.

3.2 Examples

Here, some examples are given for illustration the presented protocol without considering the eavesdropping checking. Let $N = 4$ and their privacies are $p_1 = 214$, $p_2 = 403$, $p_3 = 211$, $p_4 = 043$, respectively. The pre-shared key A among four participants is 123.

Step 1: TP randomly prepares 3×4 9-dimensional Bell states,

$$\begin{matrix} \left|\psi_{3_1^1,5_1^1}\right\rangle, \left|\psi_{2_2^1,1_2^1}\right\rangle, \left|\psi_{6_3^1,0_3^1}\right\rangle, \left|\psi_{4_4^1,4_4^1}\right\rangle \\ \left|\psi_{0_1^2,1_1^2}\right\rangle, \left|\psi_{1_2^2,3_2^2}\right\rangle, \left|\psi_{0_3^2,0_3^2}\right\rangle, \left|\psi_{6_4^2,7_4^2}\right\rangle \\ \left|\psi_{8_1^3,6_1^3}\right\rangle, \left|\psi_{2_2^3,6_2^3}\right\rangle, \left|\psi_{3_3^3,1_3^3}\right\rangle, \left|\psi_{5_4^3,7_4^3}\right\rangle \end{matrix} \tag{11}$$

First, he records $v_1^1 v_1^2 v_1^3 = 516$, $v_2^1 v_2^2 v_2^3 = 136$, $v_3^1 v_3^2 v_3^3 = 001$, $v_4^1 v_4^2 v_4^3 = 477$ according to Eq. 11. Then, he prepares a set of sequences $S' = \{S_n' | n = 1, 2, 3, 4.\}$ and sends sequence S_n' to the corresponding participant via the quantum channel.

Step 2: Suppose that no eavesdropper is detected; then, move to Step 3.

Step 3: After removing these decoy particles, Participants P_1, P_2, P_3 and P_4 will measure the remaining particles with Z basis and record the measurement results. If their measurement results are $k_1 = 203$, $k_2 = 874$, $k_3 = 257$, $k_4 = 161$, then the TP's measurement results in Step 5 can be determined according to the entanglement properties of Bell state and they are

$$t_1 = 710,\ t_2 = 011,\ t_3 = 258,\ t_4 = 548 \tag{12}$$

Therefore, after all participants encode their privacies according to Eq. 4, Participants P_1, P_2, P_3 and P_4 will obtain $c_1 = 531$, $c_2 = 401$, $c_3 = 581$,$c_4 = 237$, separately. Then, each participant will send the encoding information to TP via an authenticated channel.

Step 4: When confirming that the encoding information from all participants has been received, the TP will measure the particles in sequence $T_n (n = 1, 2, 3, 4)$. From Step 3, one can know that the TP's measurement results must be determined as Eq. 12. Therefore, after TP computes C_n^l, he will obtain $C_1 = 337$, $C_2 = 526$, $C_3 = 333$, $C_4 = 166$.

Step 5: TP will finish sorting the privacies by size as follows

$$\begin{aligned} &R_{12}^1 = \left(C_1^1 \ominus C_2^1\right) = (3 \ominus 5) = 7,\ R_{13}^1 = \left(C_1^1 \ominus C_3^1\right) = (3 \ominus 3) = 0 \\ &R_{14}^1 = \left(C_1^1 \ominus C_4^1\right) = (3 \ominus 1) = 2,\ R_{23}^1 = \left(C_2^1 \ominus C_3^1\right) = (5 \ominus 3) = 2 \\ &R_{24}^1 = \left(C_2^1 \ominus C_4^1\right) = (5 \ominus 1) = 4,\ R_{34}^1 = \left(C_3^1 \ominus C_4^1\right) = (3 \ominus 1) = 2 \end{aligned} \tag{13}$$

Similar to Eq. 13, the TP can obtain $R_{12}^2 = 1$, $R_{13}^2 = 0$, $R_{14}^2 = 6$, $R_{23}^2 = 8$, $R_{24}^2 = 5$, $R_{34}^2 = 6$, $R_{12}^3 = 1$, $R_{13}^3 = 4$, $R_{14}^2 = 1$, $R_{23}^3 = 3$, $R_{24}^2 = 0$, $R_{34}^2 = 6$. Therefore, based on Eqs 7, 8, TP can deduce the comparison results as follows

$$\begin{aligned} \text{sign}\left[R_{12}^1, R_{13}^1, R_{14}^1, R_{23}^1, R_{24}^1, R_{34}^1\right] &= \text{sign}\left[7, 0, 2, 2, 4, 2\right] \\ &= -1, 0, 1, 1, 1, 1 \\ \Rightarrow p_2^1 > p_1^1 &= p_3^1 > p_4^1 \\ \text{sign}\left[R_{12}^2, R_{13}^2, R_{14}^2, R_{23}^2, R_{24}^2, R_{34}^2\right] &= \text{sign}\left[1, 0, 6, 8, 5, 6\right] \\ &= 1, 0, -1, -1, -1, -1 \\ \Rightarrow p_4^2 > p_3^2 &= p_1^2 > p_2^2 \\ \text{sign}\left[R_{12}^3, R_{13}^3, R_{14}^3, R_{23}^3, R_{24}^3, R_{34}^3\right] &= \text{sign}\left[1, 4, 1, 3, 0, 6\right] \\ &= 1, 1, 1, 1, 0, -1 \\ \Rightarrow p_1^3 > p_2^3 &= p_4^3 > p_3^3 \end{aligned}$$

Apparently, the size relationship that TP sorts without knowing participants' privacies is consistent with the actual data ($p_1 = 214$, $p_2 = 403$, $p_3 = 211$, $p_4 = 043$) given in Section 3.2. To further clarify this process, more examples are compiled in Table 1.

4 Security analysis

Assumed that the quantum and authentical channels are the ideal channels, that's to say, there is no noise in the channel and the particles can be sent to the receivers. In this section, the security of the proposed protocol will be analyzed from both external and internal attack. It is shown that no private information has been leaked according to the security analysis.

TABLE 1 Relation of essential indices for some examples.

Initial states	$L \times N$	d	p_1	p_2	p_3	k_1	k_2	k_3	c_1	c_2	c_3	A	**sign** $[R^1_{12}, R^1_{13}, R^1_{23}]$ **sign** $[R^2_{12}, R^2_{13}, R^2_{23}]$ **sign** $[R^3_{12}, R^3_{13}, R^3_{23}]$	**Size relationship**
$\|\psi_{0^1_1,4^1_1}\rangle,\|\psi_{1^1_2,3^1_2}\rangle,\|\psi_{2^1_3,0^1_3}\rangle$	2×3	5	21	10	11	03	14	21	41	41	04	22	1, 1,0 1, 0,−1	$p^1_1 > p^1_2 = p^1_3$ $p^2_1 = p^2_3 > p^2_2$
$\|\psi_{3^2_1,2^2_1}\rangle,\|\psi_{1^2_2,4^2_2}\rangle,\|\psi_{3^2_3,4^2_3}\rangle$			01	12	20	22	43	34	43	20	24	20	−1,−1,−1 −1, 1, 1	$p^1_3 > p^1_2 > p^1_1$ $p^2_2 > p^2_1 > p^2_3$
$\|\psi_{1^1_1,2^1_1}\rangle,\|\psi_{0^1_2,3^1_2}\rangle,\|\psi_{2^1_3,4^1_3}\rangle$ $\|\psi_{3^2_1,5^2_1}\rangle,\|\psi_{6^2_2,1^2_2}\rangle,\|\psi_{3^2_3,4^2_3}\rangle$	3×3	9	123	014	201	321	382	601	448	301	806	004	1,−1,−1 1, 1, 1 −1, 1, 1	$p^1_3 > p^1_1 > p^1_2$ $p^2_1 > p^2_2 > p^2_3$ $p^3_2 > p^3_1 > p^3_3$
$\|\psi_{5^3_1,6^3_1}\rangle,\|\psi_{2^3_2,0^3_2}\rangle,\|\psi_{4^3_3,1^3_3}\rangle$			401	432	210	372	616	064	885	251	386	112	0, 1, 1 −1,−1,1 −1, 1, 1	$p^1_1 = p^1_2 > p^1_3$ $p^2_2 > p^2_3 > p^2_1$ $p^3_2 > p^3_1 > p^3_3$
$\|\psi_{5^1_1,6^1_1}\rangle,\|\psi_{6^1_2,5^1_2}\rangle,\|\psi_{5^1_3,4^1_3}\rangle$ $\|\psi_{6^2_1,5^2_1}\rangle,\|\psi_{4^2_2,1^2_2}\rangle,\|\psi_{4^2_3,3^2_3}\rangle$ $\|\psi_{5^3_1,0^3_1}\rangle,\|\psi_{2^3_2,3^3_2}\rangle,\|\psi_{4^3_3,2^3_3}\rangle$	3×3	7	103	201	312	314	240	616	423	453	233	012	−1,−1,−1 0,−1,−1 1, 1,−1	$p^1_3 > p^1_2 > p^1_1$ $p^2_3 > p^2_2 = p^2_1$ $p^3_1 > p^3_3 > p^3_2$
			310	220	032	646	302	161	302	645	246	123	1, 1, 1 −1,−1,−1 0, −1, −1	$p^1_1 > p^1_2 > p^1_3$ $p^2_3 > p^2_2 > p^2_1$ $p^3_3 > p^3_2 = p^3_1$

10.3389/fphy.2022.981376

4.1 External attack

Eve, an external attacker, may attempt to acquire information from the participants including TP. In Step 1, Sequence $S_n^{'}$ is sent to the corresponding participant via the quantum channel. Eve may steal some useful information from sequences $S_n^{'}$ with many kinds of attacks in this step. Obviously, the security of the protocol is guaranteed by inserting the decoy particles [21, 22]. Since Eve does not know the position and the measurement basis of each decoy particle, some well-known attacks, such as intercept-resend attack, measurement-resend attack, and entanglement-measure attack can be detected with the checking mechanism [4, 23, 24]. The decoy particle technology can be thought as a variant of the eavesdropping check method of the BB84 protocol [25] which has been proven to provide unconditionally security [26]. In Step 2, the encoding information is sent to the TP via the authenticated channels. The security in this step is promised. Therefore, an external attacker cannot learn any useful information about the privacies without being detected.

4.2 Internal attack

Case 1 Internal attack from P_n

Suppose participant P_n is a dishonest participant who tries to obtain other participants' privacies in Step 1. Since P_n has no knowledge about the positions and the measurement bases of counterparts' decoy particles, the attack from the participant P_n will be detected as an external one as described in Section 4.1. Thus, the proposed protocol is immune to internal attack from dishonest P_n.

Case 2 Internal attack from TP

From Section 2.2, one can know that TP is both the sender of quantum information and the receiver of all encrypted information. Therefore, he can obtain more information than other attackers during the protocol execution. Significantly, due to TP semi-honesty, that the only thing he can do is try to extract the information from the received ciphertext $c_n^l = k_n^l \oplus p_n^l \oplus A^l$. However, he is unable to learn any information about A^l shared among these participants with a secure QKD protocol. Thus, the TP can't obtain any useful private information from c_n^l with the internal attack.

5 Discussion

In Table 2, the proposed protocol is compared with some other similar protocols with the following aspects: quantum resource used, category of QPC (size or equality), number of participants, number of TP, need for the authenticated classical channel, need for unitary operation, measurement involved, and qubit efficiency η (Defined as $\eta = b_c/b_t$, where b_c is the total number of compared qubit while b_t is the total number of qubits and classical bits used in this protocol).

In Ref. [27], we proposed a new QPC protocol to compare the size relationship of privacies between two participants. The quantum resources used in the protocol are d-dimensional GHZ states. To calculate the qubit efficiency η, we must count the number of bits consumed in the transmission of information. First, TP needs $12L$ (L is the length of each privacy) qubits to prepare $4L$ GHZ states. Second, the participants (Alice and Bob) use $4L$ qubits to send information to the TP. $2L$ is the total number of compared qubit. Hence, the qubit efficiency is $\eta = 1/8$. It is noted that the protocol can only make private comparison between two participants. In addition, both Bell measurement and single-particle measurement are needed.

In Ref. [28], the authors presented a new QPC protocol to compare the equality of privacies between two participants. The quantum resources used are GHZ states. First, the TP needs $8L$ qubits to prepare L four-particle GHZ states and $4L$ decoy states. Second, Alice needs $2L$ qubits to send information to Bob. Third, Alice and Bob need $2L$ qubits to send information to the TP. In addition, the total number of compared qubit is $2L$. Hence, the qubit efficiency is $\eta = 1/6$. In

TABLE 2 The comparisons of our QPC with other similar QPC protocols.

Compared aspects	Reference [27]	Reference [28]	Reference [29]	Reference [30]	Our protocol
Quantum resources	dD GHZ state	GHZ state	dD GHZ state	GHZ state	dD Bell state
Category of QPC	Size	Equality	Size	Equality	Size
Number of participants	2	2	N ($N \geq 2$)	N ($N \geq 2$)	N ($N \geq 2$)
Number of TP	1	1	1	2	1
Efficiency η	$\frac{1}{8}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{4}$
Need for authenticated classical channels	No	Yes	No	Yes	Yes
Need for unitary operation	No	Yes	Yes	No	No
measurement	BM and SM	BM and SM	SM	SM	SM

SM (single-particle measurement), BM (Bell measurement), dD (d-dimensional).

the protocol, both Bell measurement and single-particle measurement are involved, and unitary operation is needed.

In Ref. [29], a novel MQPC protocol for comparing the size relationship among N participants' privacies was designed. The quantum resources used are d-dimensional GHZ states. First, the TP needs $4NL$ qubits to prepare L pairs of N-particle d-dimensional GHZ states and $2NL$ decoy states. Second, each participant needs $2L$ qubits to sends information to the TP. Thus, $b_t = 4NL + 2NL$. In addition, the total number of compared bits b_c is NL. Hence, the qubit efficiency is $\eta = 1/6$. Although the authenticated channels are not necessary in advance, quantum unitary operations have to be performed in the protocol.

In Ref. [30], the authors proposed a new MQPC protocol to compare the size relationship among N participants' privacies. The quantum resources used are N-particle GHZ states. First, the TP_1 needs $2NL$ qubits to prepare L N-particle GHZ states and NL decoy states. It is note that TP_1 sends the information of the initial GHZ states to TP_2 using quantum secure direct communication protocol. Second, each participant needs $2L$ classical bits to send information to TP_1 and TP_2 via the authenticated channels. The total number of compared qubit is NL. Hence, the qubit efficiency is $\eta = 1/4$. In addition to the classic authentication channels, two TPs are required in the protocol.

In our protocol, a new MQPC protocol to compare the size relationship among N participants' privacies was proposed. The quantum resources used are d-dimensional Bell states. First, the TP_1 needs $3NL$ qubits to prepare NL d-dimensional Bell states and NL decoy particles. Second, each participants need L classical bits to send information to the TP via the authenticated classical channel. The total number of compared qubit is NL. Hence, the qubit efficiency is $\eta = 1/4$.

From Table 2, one can see that, like the protocols in [27, 29], our protocol can compare the size relationship among privacies, while in [28, 30] they can only compare the equality. When it comes to the MQPC, Refs. [27, 28] are useless. Compared with these protocols listed in Table 2, the unitary operation is not necessary, and only single-particle measurement is required in our protocol. Additionally, our protocol ensures the highest qubit efficiency only with the help of one TP. Table 2 clearly shows that the performance of the proposed protocol is better than these similar QPC protocols. However, it has to be said that the high dimensional quantum state is not easy to obtain experimentally at present. Therefore, we still need to work harder to realize the protocol based on the high dimensional quantum state in experiment.

6 Conclusion

Based on the d-dimensional Bell states, a novel MQPC protocol is presented. With the help of a semi-honest quantum TP, our protocol can determine the size relationship among N participants' privacies without any information leakage. Since the quantum measurement and unitary operation aren't required, it is easier to implement the proposed protocol. Furthermore, compared with the similar protocols, the qubit efficiency is increased. Decoy particles promise the security of the proposed protocol. Although it will take many efforts to move the theoretical research towards social practices, we will be very happy if this work plays a little facilitating role in further research of QSMC.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

BW: Conceptualization, methodology, investigation, formal analysis, writing—original draft; L-HG: validation, writing- reviewing and editing S-QL: Conceptualization, funding acquisition, resources, supervision, writing—review and; editing.

Funding

This work is supported by the National Natural Science Foundation of China Grant No. 62161025, the Project of Scientific and Technological Innovation Base of Jiangxi Province Grant No. 20203CCD46008, and the Jiangxi Provincial Key Laboratory of Fusion and Information Control Grant No. 20171BCD40005.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

1. Yao AC. Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (SFCS'08); 03-05 November 1982. Washington, DC, USA: IEEE (1982). p. 160–4. doi:10.1109/SFCS.1982.38

2. Boudot F, Schoenmakers B, Traore J. A fair and efficient solution to the socialist millionaires' problem. *Discrete Appl Math* (2001) 111:23–36. doi:10.1016/s0166-218x(00)00342-5

3. Lo HK. Insecurity of quantum secure computations. *Phys Rev A (Coll Park)* (1997) 56:1154–62. doi:10.1103/physreva.56.1154

4. Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J Phys A: Math Theor* (2009) 42:055305. doi:10.1088/1751-8113/42/5/055305

5. Chen XB, Xu G, Niu XX, Wen QY, Yang YX. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. *Opt Commun* (2010) 283:1561–5. doi:10.1016/j.optcom.2009.11.085

6. Jia HY, Wen QY, Song TT, Gao F. Quantum protocol for millionaire problem. *Opt Commun* (2011) 284:545–9. doi:10.1016/j.optcom.2010.09.005

7. Lin S, Sun Y, Liu XF, Yao ZQ. Quantum private comparison protocol with d-dimensional Bell states. *Quan Inf Process* (2013) 12:559–68. doi:10.1007/s11128-012-0395-6

8. Chang YJ, Tsai CW, Hwang T. Multi-user private comparison protocol using GHZ class states. *Quan Inf Process* (2013) 12:1077–88. doi:10.1007/s11128-012-0454-z

9. Luo QB, Yang GW, She K, Niu WN, Wang YQ. Multi-party quantum private comparison protocol based on $$d$$ d -dimensional entangled states. *Quan Inf Process* (2014) 13:2343–52. doi:10.1007/s11128-014-0805-z

10. Wang QL, Sun HX, Huang W. Multi-party quantum private comparison protocol with $$n$$ n -level entangled states. *Quan Inf Process* (2014) 13:2375–89. doi:10.1007/s11128-014-0774-2

11. Zhang B, Liu XT, Wang J, Wang J, Tang CJ. Cryptanalysis and improvement of quantum private comparison of equality protocol without a third party. *Quan Inf Process* (2015) 14:4593–600. doi:10.1007/s11128-015-1145-3

12. Ji ZX, Zhang HG, Fan PR. Two-party quantum private comparison protocol with maximally entangled seven-qubit state. *Mod Phys Lett A* (2019) 34:1950229. doi:10.1142/s0217732319502298

13. Zhou NR, Xu QD, Du NS, Gong LH. Semi-quantum private comparison protocol of size relation with d-dimensional Bell states. *Quan Inf Process* (2021) 20:124. doi:10.1007/s11128-021-03056-6

14. Liu W, Wang YB, Wang XM. Quantum multi-party private comparison protocol using d-dimensional bell states-dimensional bell states. *Int J Theor Phys (Dordr)* (2015) 54:1830–9. doi:10.1007/s10773-014-2388-y

15. Ye CQ, Ye TY. Multi-party quantum private comparison of size relation with d-level single-particle states-level single-particle states. *Quan Inf Process* (2018) 17:252. doi:10.1007/s11128-018-2021-8

16. Cao H, Ma WP, Lü LD, He YF, Liu G. Multi-party quantum privacy comparison of size based on d-level GHZ states. *Quan Inf Process* (2019) 18:287. doi:10.1007/s11128-019-2401-8

17. Ye TY, Hu JL. Multi-party quantum private comparison based on entanglement swapping of bell entangled states within d-level quantum system. *Int J Theor Phys (Dordr)* (2021) 60(4):1471–80. doi:10.1007/s10773-021-04771-7

18. Daniel BS, Constantin B, Patrick JC, Norbert L, Ryan MC, Junji U, et al. Self-referenced continuous-variable quantum key distribution protocol. *Phys Rev X* (2015) 5:041010. doi:10.1103/physrevx.5.041010

19. Liu XS, Long GL, Tong DM, Li F. General scheme for super dense coding between multi-parties. *Phys Rev A (Coll Park)* (2002) 65:022304. doi:10.1103/physreva.65.022304

20. Liu ZH, Chen HW, Xu J, Liu WJ, Li ZQ. High-dimensional deterministic multiparty quantum secret sharing without unitary operations. *Quan Inf Process* (2013) 11:1785–95. doi:10.1007/s11128-011-0333-z

21. Lo HK, Ma X, Chen K. Decoy state quantum key distribution. *Phys Rev Lett* (2005) 94:230504. doi:10.1103/PhysRevLett.94.230504

22. Wang XB. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys Rev Lett* (2005) 94:230503. doi:10.1103/PhysRevLett.94.230503

23. Deng FG, Li XH, Zhou HY. Efficient high-capacity quantum secret sharing with two-photon entanglement. *Phys Lett A* (2008) 372(12):1957–62. doi:10.1016/j.physleta.2007.10.066

24. Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A (Coll Park)* (2003) 68(4):042317. doi:10.1103/physreva.68.042317

25. Bennett CH, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing; 14-16 Nov. 2005. Bangalore. India: IEEE Press (1984). p. 175–9.

26. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett* (2000) 85(2):441–4. doi:10.1103/physrevlett.85.441

27. Wang B, Liu SQ, Gong LH. Semi-quantum private comparison protocol of size relation with d-dimensional GHZ states. *Chin Phys B* (2022) 31:010302. doi:10.1088/1674-1056/ac1413

28. Xu QD, Chen HY, Gong LH, Zhou NR. Quantum private comparison protocol based on four-particle GHZ states. *Int J Theor Phys (Dordr)* (2020) 59:1798–806. doi:10.1007/s10773-020-04446-9

29. Huang SL, Hwang T, Gope P. Multi-party quantum private comparison with an almost-dishonest third party. *Quan Inf Process* (2015) 14:4225–35. doi:10.1007/s11128-015-1104-z

30. Hung SM, Huang SL, Hwang T, Kao SH. Multiparty quantum private comparison with almost dishonest third parties for strangers. *Quan Inf Process* (2017) 16:36. doi:10.1007/s11128-016-1498-2